A3222-Q56

SHA256 Processor

Datasheet

Version 0.1

June. 27th, 2014

Notes1: The information is subject to change without notice. Before using this document, please confirm that this is the latest version.
Notes2: Not all products and/or types are available in every country. Please check with sales representative for availability and additional information.

Table of Content

1. GENERAL DESCRIPTION

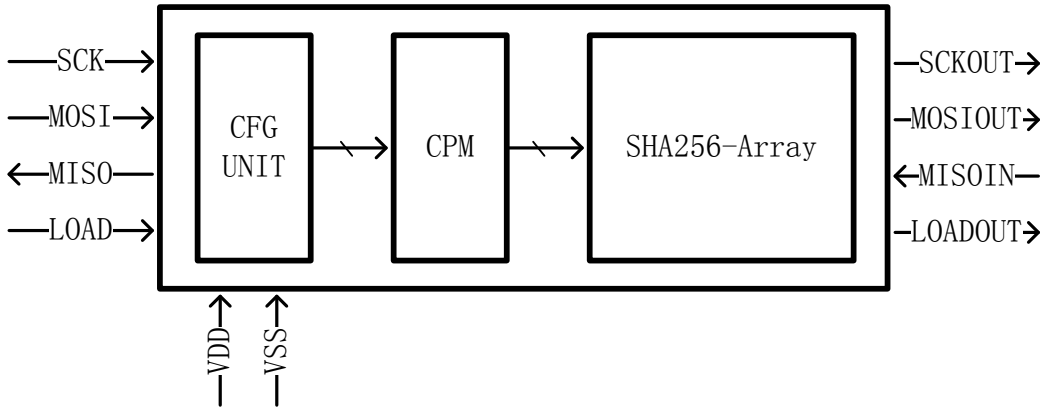
A3222Q56 is the fourth generation SHA256 Processor designed by AVALON team, comes with higher hash speed and performance per watt. The major applications for this chip is provide a chip level solution for SHA256 related work.

Features

- Communication protocol compatible with the serial peripheral interface (SPI).
- Support chain-mode, drastically reduced controller I/O port requirement.
- More efficient clock strategy.
- Efficient data transfer with two levels of frame buffer.

2. SYSTEM ARCHITECTURE

Figure 2-1 Chip Architecture



3. DATA INTERFACE

3.1 Communication Protocol

A3222Q56 interface supports SPI mode0: CPOL = 0, CPHA = 0. Input data is latched in on the rising edge of SCK, and output data is available from the falling edge of SCK.

When the bus master is in standby mode: SCK remains at 0 for (CPOL = 0, CPHA = 0 Mode 0). All timing diagrams shown in this data sheet are mode 0.

3.2 Communication Port

A3222Q56 uses 2 pairs of communication ports to receive configurations and transmit the configurations to the chip at next stage and send out the calculation result, details are listed in Table 3-1.

Figure 3-1 A3222Q56 Communication Topology

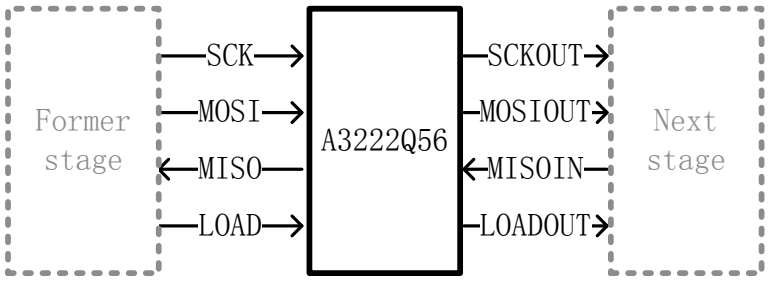
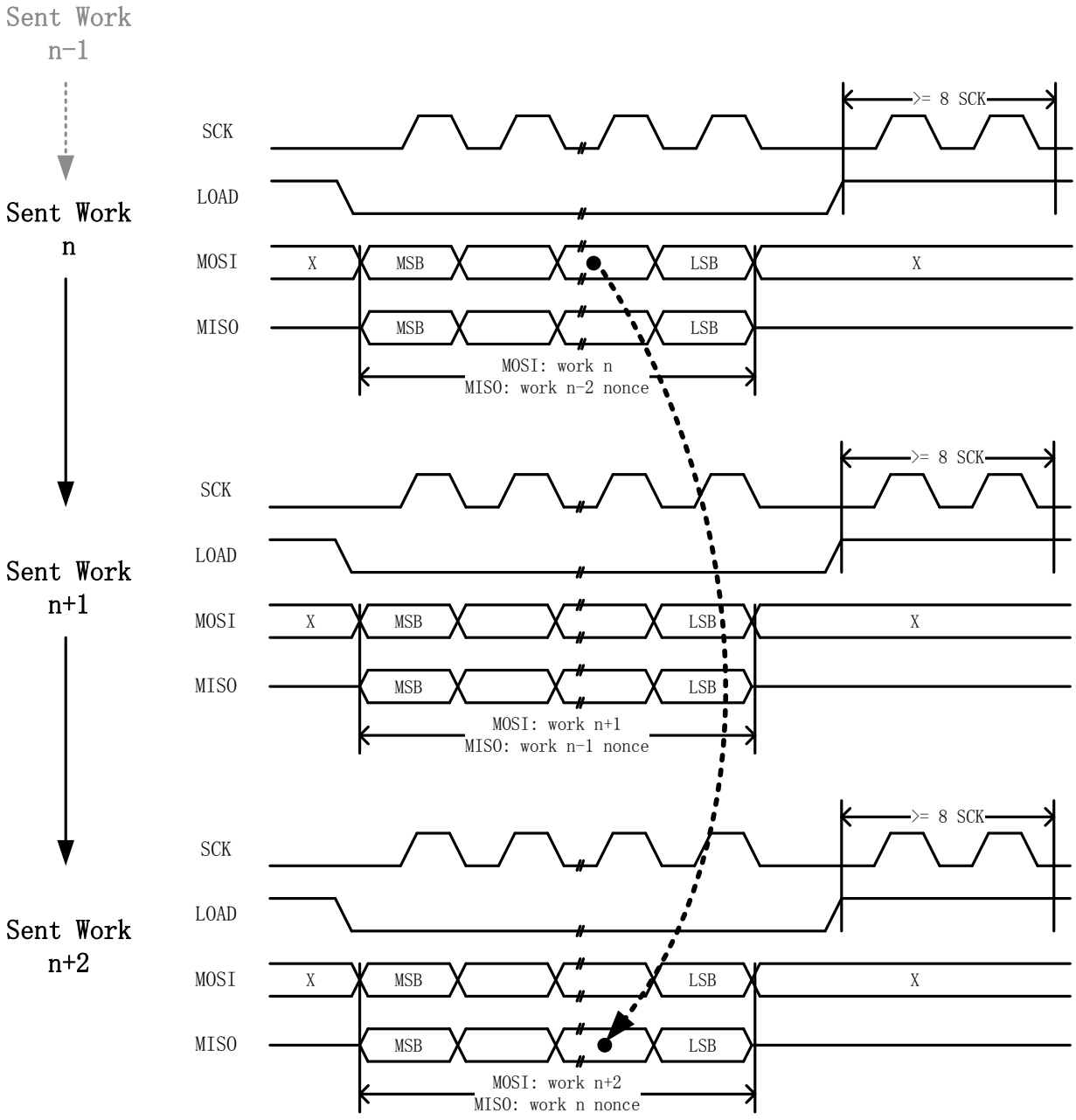


Table 3-1 A3222Q56 Communication Port, former stage/next stage

PIN NAME	FUNCTION
LOAD/LOADOUT	End of frame. When LOAD goes LOW, the device is placed in active mode. When LOAD is HIGH, the device is placed in inactive mode. **Note**: While LOAD is HIGH, Still need to send at least 8 SCK (unlike the mode 0). PINS: LOAD: from former state. LOADOUT: to next stage.
MISO/MISOIN	Send out the golden nonce when A3222Q56 get the share. Data is placed on MISO at the falling edge of SCK. PINS: MISO: to former stage. MISOIN: from next stage.
MOSI/MOSIOUT	Receive configurations from controller or another A3222Q56 chip. Data is placed on MISO at the falling edge of SCK.

	PINS: MOSI: from former stage. MOSIOUT: to next stage.
SCK/SCKOUT	Serial clock provides interface timing for the chip. PINS: SCK: from former stage. SCKOUT: to next stage.

Figure 3-2 A3222Q56 Communication Example

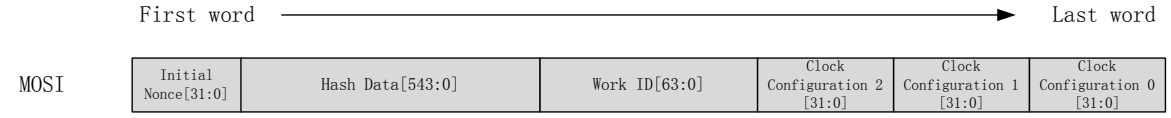


NOTE:
(1) While LODE is HIGH, Still need to send at least 8 SCK (unlike the mode 0).
(2) A A3222Q56-work frame is 736bits.
(3) The current report is twice the previous work.
ie: MISO(n) = SHA256(MOSI(n-2)).

4. DATA FORMAT

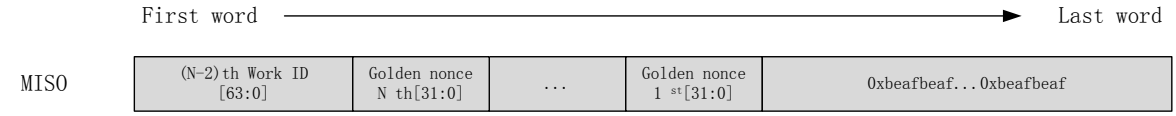
Three segments should be configured before A3222Q56 hash calculation by MISO. Clock configuration segment is for adjusting clock frequency, gating core clock or switching clock source. Hash data segment is the initial input data of SHA256 HASH. Hash work of chips in the same chain is split by the initial nonce segment. Configure data should send as the order shown in Figure 4-1

Figure 4-1 A3222Q56 Configure Sequence



When A3222Q56 get nonce, it will return nonce and work ID by a SPI read process.

Figure 4-2 A3222Q56 Receive golden nonce and Work ID Sequence



NOTE:
(1) 0xbeafbeaf in nonce report zone should be ignored.
(2) All input/output data is 32bit aligned, and send out in MSB (that means lowest bit send first).

4.1 Clock Configuration Segment

Clock configuration segment has two words (1word=32bit), detail information of each bit listed below.

Bit[0]:Reserved, should be 1.

Bit[1]:clock configuration effect bit, if this bit is 0, all clock configuration at current transaction is ineffective.

Bit[2]:clock frequency effect bit, set to 1 if there are clock divider changes.

Bit[3]:clock gate, hash unit working clock will be gated it set to 1.

Bit[4]: Reserved, should be 0.

bit[5]:clock switch, hash unit working clock will switch to XCLKIN if set to 1.

Bit[6]:enable/disable core clock output to PAD, when set to 1, core clock output to PAD CORE_CLOCKOUT is disabled.

Bit[9:7]:PLL output divider; 0: PLL/1, 1: PLL/2, 2: PLL/4, 3: PLL/8, 4:

PLL/16, 5: PLL/32, 6: PLL/64, 7: PLL/128;

Bit[10]: Select internal feedback path.

Bit[14:11] :NR = CLKR[3:0] + 1, CLKR[0] is LSB.

Bit[20:15] :NF = CLKF[5:0] + 1, CLKF[0] is LSB.

Bit[24:21] :OD = CLKOD[3:0] + 1, CLKOD[0] is LSB.

Bit[30:25] :Loop BW adj.: NB = BWADJ[5:0] + 1, BWADJ[0] is LSB.

Bit[31]: Reference-to-output bypass when high.

The output frequency Fout at CLKOUT is related to the reference frequency (25M).

Fref by: Fout = Fref * NF / NR * Next

4.2 HASH Data Segment

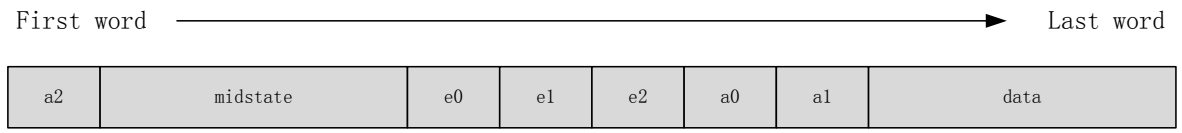
To reduce cost and get higher speed, A3222Q56 put some pre-calculation out of the chip. Controller need to do this calculation and send the result to A3222Q56. Part of code is list below in pseudo code:

```
    void
    functionpre_calc
    for(i=0;i<64;i++)
    {
       t1=h+E1(e)+CH(e,f,g)+K[i]+w[i];
       t2=E0(a)+MAJ(a,b,c);
       h=g;
       g=f;
       f=e;
       e=d+t1;
       d=c;
       c=b;
       b=a;
       a=t1+t2;
        if(i=0) a0 = a;
        if(i=1) a1 = a;
        if(i=2) a2 = a;
        if(i=0) e0 = e;
        if(i=1) e1 = e;
        if(i=2) e2 = e;
  }
```

a0, a1, a2, e0, e1, e2 is the pre-calculation result should send to A3222Q56 (for further information, please refer to http://en.wikipedia.org/wiki/SHA256).

The complete sequence of Hash Data Segment is shown in Figure 4-3

Figure 4-2 Hash Data Segment Transfer Sequence



All data is sent in MSB, means high bit, high byte and high word is sent first

4.3 Receive Nonce

The REAL golden nonce and the received nonce satisfy the following equals:

Golden nonce = Received nonce – 0x1000

672 bits nonce and 64 bits work ID will be read out, and the data format see Figure 4-2.

Controller should save the whole hash data and match the result to work received. (AN example of receive nonce: Figure 3-2 A3222Q56 Communication Example)

5. PIN ASSIGNMENTS

Signal Type	Description
P	Power/Ground
I	Input
O	Output
PU	Internal pull-up resistor
PD	Internal pull-down resistor
/	Multi-function separator
NC	Not Connect

5.1 System Control

PIN NO.	PAD NAME	TYPE	FUNCTION
6	RSTN	I,PU	Hardware Reset signal, low voltage active.
10	XCLKIN	I	Crystal Clock input to chip
30	TEST	O	Debug Clock output from chip

5.2 Function

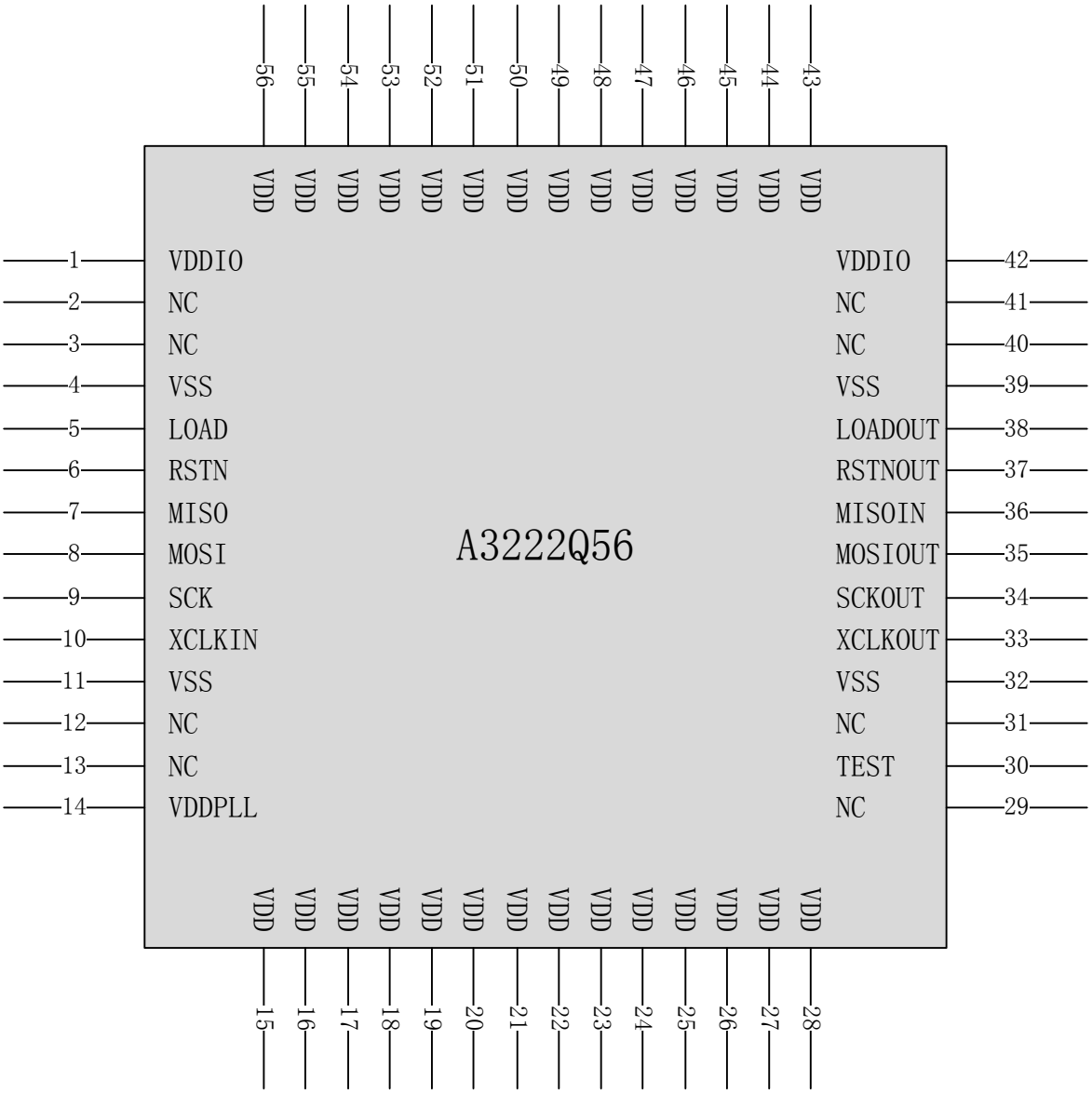
PIN NO.	PAD NAME	TYPE	FUNCTION
5	LOAD	I, PD	End of frame. See Table 3-1.
7	MISO	O	Send out the golden nonce when A3222Q56 get the share.
8	MOSI	I, PD	Receive configurations from controller or another A3222Q56 chip.
9	SCK	I, PD	Serial clock provides interface timing for the chip.
34	SCKOUT	O	SCK to next stage.
35	MOSIOUT	O	Internal work buffer to next stage.
36	MISOIN	I, PD	Report data from next stage.
38	LOADOUT	O	LOAD to next stage.

5.3 Power Supply

PIN NO.	PAD NAME	TYPE	FUNCTION
1	VDDIO	P	1.8V IO Power
2	NC	NC	Not Connect
3	NC	NC	Not Connect
4	VSS	P	0.9V Ground
11	VSS	P	0.9V Ground
12	NC	NC	Not Connect
13	NC	NC	Not Connect
14	VDDPLL	P	0.9V PLL Power
15	VDD	P	0.9V Core Power
16	VDD	P	0.9V Core Power
17	VDD	P	0.9V Core Power
18	VDD	P	0.9V Core Power
19	VDD	P	0.9V Core Power
20	VDD	P	0.9V Core Power
21	VDD	P	0.9V Core Power
22	VDD	P	0.9V Core Power
23	VDD	P	0.9V Core Power
24	VDD	P	0.9V Core Power
25	VDD	P	0.9V Core Power
26	VDD	P	0.9V Core Power
27	VDD	P	0.9V Core Power
28	VDD	P	0.9V Core Power
29	NC	NC	Not Connect
31	NC	NC	Not Connect
32	VSS	P	0.9V Ground
39	VSS	P	0.9V Ground
40	NC	NC	Not Connect
41	NC	NC	Not Connect
42	VDDIO	P	1.8V IO Power
43	VDD	P	0.9V Core Power

44	VDD	P	0.9V Core Power
45	VDD	P	0.9V Core Power
46	VDD	P	0.9V Core Power
47	VDD	P	0.9V Core Power
48	VDD	P	0.9V Core Power
49	VDD	P	0.9V Core Power
50	VDD	P	0.9V Core Power
51	VDD	P	0.9V Core Power
52	VDD	P	0.9V Core Power
53	VDD	P	0.9V Core Power
54	VDD	P	0.9V Core Power
55	VDD	P	0.9V Core Power
56	VDD	P	0.9V Core Power

5.4 A3222Q56 Pin-Pad Map



6. ELECTRICAL CHARACTERISTICS

6.1 Recommended Operating Conditions

The recommended operating conditions are the recommended values to assure normal logic operation. As long as the device is used within the recommended operating conditions, the electrical characteristics (DC and AC characteristics) described below are assured.

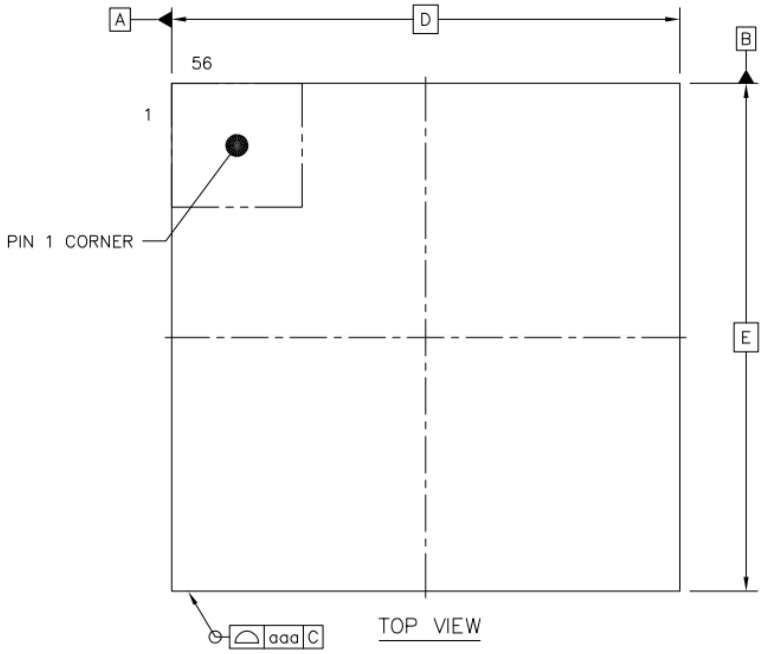
PARAMETER.	SYMBOL	MIN	TYP	MAX	UNIT
Supply Core voltage	DVDD	0.75	0.75	0.9	V
Supply 1.0V analog voltage	VDDA_PLL	0.9	0.9	1.0	V
Supply I/O voltage	OVDD	1.8	1.8	1.8	V
Maximum input voltage	$V_{i\max}$	--	--	0.9	V
Operating Temperature	T_{OPR}	-20	--	+85	℃
Storage Temperature	T_{STOR}	-40	--	+125	℃
Operating Current	I_{OP}	--	--	TBD	mA
Static Current	I_{SUSP}	--	--	20	mA

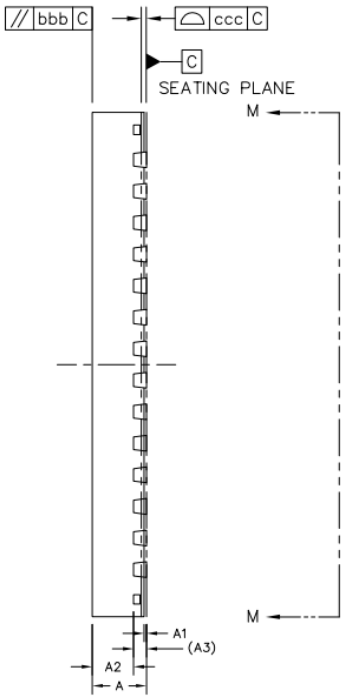
6.2 Oscillation

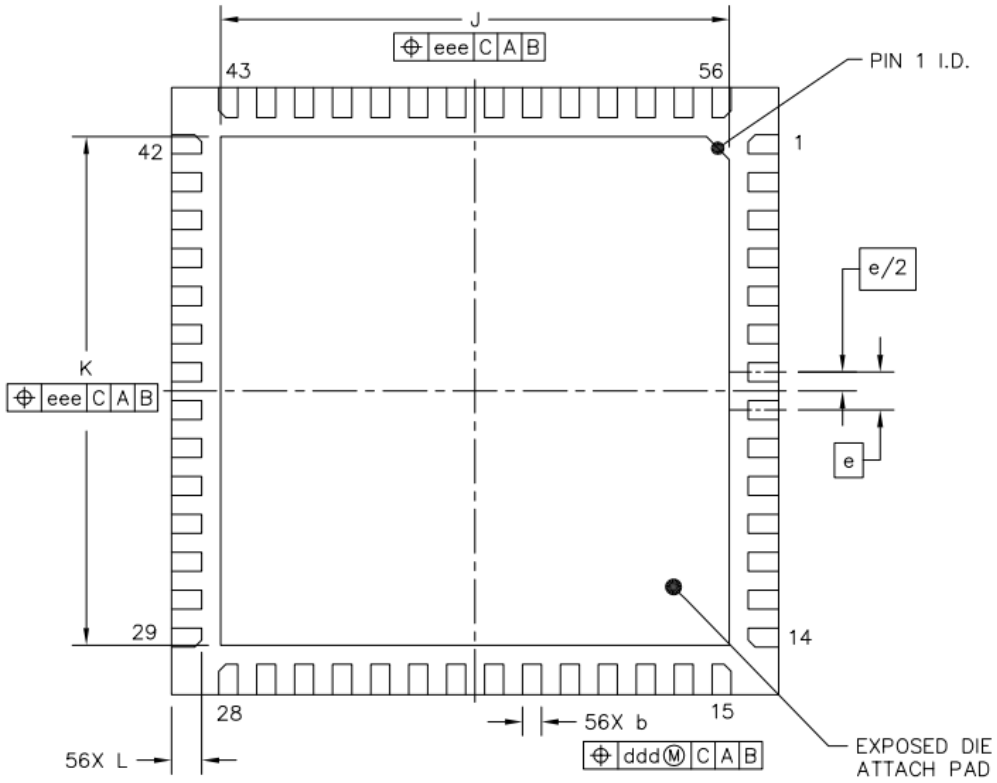
PARAMETER.	CONDITIONS	SYMBOL	MIN	TYP	MAX	UNIT
Input clock frequency	--	Fclixin	--	25	--	MHz
Input clock period	--	Tclkxin	--	40	--	Ns
Clock duty cycle	--	--	45	50	55	%
Input pad capacitance	--	--	--	3.398	--	Pf
Jitter	--	--	--	--	10	Ps
Input HIGH leakage current	--	--		--	±10	uA
Input LOW leakage current	--	--	--	--	±10	uA

7. PACKAGE INFORMATION

7.1 A3222Q56 Package Specifications







BOTTOM VIEW
VIEW M–M

		SYMBOL	MIN	NOM	MAX
TOTAL THICKNESS		A	0.8	0.85	0.9
STAND OFF		A1	0	0.035	0.05
MOLD THICKNESS		A2	---	0.65	---
L/F THICKNESS		A3		0.203 REF	
LEAD WIDTH		b	0.2	0.25	0.3
BODY SIZE	X	D		8 BSC	
	Y	E		8 BSC	
LEAD PITCH		e		0.5 BSC	
EP SIZE	X	J	6.6	6.7	6.8
	Y	K	6.6	6.7	6.8
LEAD LENGTH		L	0.35	0.4	0.45
PACKAGE EDGE TOLERANCE		aaa		0.1	
MOLD FLATNESS		bbb		0.1	
COPLANARITY		ccc		0.08	
LEAD OFFSET		ddd		0.1	
EXPOSED PAD OFFSET		eee		0.1	

8. REVISION HISTORY

Version No.	Remarks	Release Date
0.1	Initial version released for engineering review.	2014-06-27